Written Statement from Victoria M. Prescott, representing Regenstrief Institute, Inc.
For the AHIC's Confidentiality, Privacy and Security Workgroup Meeting on June 22, 2007

Thank you for the opportunity to provide input into your recommendation process on these important privacy matters. I was asked to address certain questions regarding the potential application of HIPAA Privacy and Security Rules directly to health information exchange (HIE) organizations and provide a working exchange's perspective for consideration. It may be helpful if I provide an overview of how the Indiana Network for Patient Care (INPC) is structured and operates today. Then, I will discuss some thoughts on the questions posed.

Overview of INPC

The INPC is a virtual HIE that was created in 1996. It was formed through a standard contract called the INPC Participation Agreement. Regenstrief Institute created the software that runs the INPC, is the administrator of the network, standardizes the data, and serves as the custodian of the data used in the INPC. The INPC Participation Agreement lays out the categories of data to be submitted to the INPC and the permitted uses of the data. Those uses include the HIPAA-defined terms: treatment, payment, healthcare operations, as well as research and public health. The agreement also established a management committee to make decisions, such as approving new members, approving research proposals, as well as giving guidance to Regenstrief on new specific uses of the data within the more broadly defined categories (e.g., quality measurement, public health uses).

Typically, the INPC participants (other than Regenstrief) are all covered entities under HIPAA. Thus, the INPC Participation Agreement includes business associate provisions, making Regenstrief the business associate of each of the participating covered entities. The agreement also requires the INPC covered entities to include language in their privacy policies that covers the INPC uses of the data.

The INPC agreement is structured so that Regenstrief is **not** dealing directly with the patients. By design, the participants wanted to maintain the direct relationship with the patient (their customers). Thus, Regenstrief does not have a privacy notice, and any requests from patients to access, amend or restrict their data would automatically be referred to the relevant INPC covered entity. Further, the INPC covered entity has agreed to consult with Regenstrief in the event it should decide to grant the patient's request to ensure such request was technologically feasible. Typically, the originating data source (e.g., hospital lab) would send an amendment in an HL7 message and the record would be electronically amended automatically. In summary, Regenstrief, as a business associate, cooperates with the covered entity with regard to individuals' rights, but Regenstrief is **not** the primary contact for the patient.

Current INPC participants include a number of hospital systems, some large practices, and several payers. The Indiana State Department of Health is also finalizing their INPC membership. There are other data sources that contribute data to the INPC but do not necessarily need data from INPC, and those are typically handled through other contractual relationships between Regenstrief and the data source (e.g., private labs, RxHub, Indiana Medicaid). To give you an idea of the scope, the INPC currently has more than 95 incoming data feeds with more than 5,000,000 clinical messages total per month, which covers approximately 1.6 million patients in the central Indiana region (25% of the state of Indiana).

Questions Being Considered At Today's Meeting

The questions that I received from ONC seem to imply there is a belief by some that there is not a "level playing field" between covered entities and non-covered entities involved in health information exchange and that expanding HIPAA or passing some other law that applies to non-covered entities is being considered. The form that such a change would take was not clear. I am not sure whether attempting to define a "health information exchange organization" and then adding them to the definition of a "covered entity" under HIPAA was being proposed or if creating some other new law to impose certain privacy and security requirements on such an entity was being recommended. In addition, I was also not clear whether direct government enforcement was being recommended. So, I will address these points in general and will be brief, especially given the time allotted.

I strongly recommend against HIPAA being extended to directly apply to health information exchange organizations for the following reasons:

1. **The current business associate model is effective and still protects privacy.** The current business associate structure for a health information exchange is working well. I am not aware of any advantages that non-covered entities have with respect to the confidentiality of the data. The HIE is **NOT** free to do whatever it wants with the data it receives from covered entities. The business associate can only do what the covered entity has allowed it to do with the data, and nothing more. Direct government oversight is not necessary, because the HIE has the business incentive of the fear of losing its data source contracts if it does not ensure confidentiality of the data. Such fear is far more influential than the fear of government enforcement. Also, the business associate agreements typically are *more* restrictive than HIPAA on the business associate's permitted uses of the data. This is generally driven by the covered entity's desire to maintain control of its data. One example of this is the public policy disclosures. The HIE generally would have to go back to each covered entity to get permission to do any sort of public policy disclosure. Another example is the restriction in our INPC Agreement not permitting use of the data for any comparison between participants (e.g., patient volumes).

2. **Government oversight is not needed and changing the playing field to cause fledgling health information exchanges all over the country to now be subject to HIPAA and its civil and criminal penalties would have a significant impact on**

the viability of those efforts. The proponents of those efforts (often themselves covered entities) may be less inclined to participate and risk additional exposure. We are already having enough difficulty in this country getting participation from covered entities without giving them another reason not to share their data. In addition, it is unknown how much additional financial burden this would cause to such fledgling HIE entities. Likely the biggest problem facing the health care sector in this regard is the financial sustainability of the health information exchange. Adding this additional financial (and criminal) risk to the equation would be detrimental and would not move the nation toward interoperability.

3. **Most health information exchanges do not deal directly with patients.** Thus, there is no need for the HIPAA provisions such as privacy notice and the individual rights (e.g., access, amend, request restrictions, and accounting for disclosures), because they are not directly applicable and this would take control of the data out of the hands of the covered entity that generated the data. The HIE has a copy of the data from the data source. The HIE does not change the data, except to standardize it. It only makes sense to have the original source of the data the one responsible for these interactions with the patient. In addition, the HIE often does not want the burden of dealing directly with the patient, which can significantly increase its costs.

Alternate Proposal: I would like to suggest one proposal to try to accommodate the intent and/or theme of some of the discussions and the concerns of some of the workgroup. I would suggest that if the HIE organization does deal directly with the patient, then it would make sense to consider having HIPAA apply to such an organization. One example could be in the case of a PHR that is populated by the patient (as opposed to just being a copy of the claims data from a covered entity health plan). In that case, the provisions of HIPAA such as privacy notice and individual rights would be relevant, because the entity has a direct relationship to the patient.

Side Note: Such a proposal could also be drafted to go one step further and include all organizations or individuals that are health care providers (that provide treatment to the patient) to be subject to HIPAA, instead of just those health care providers who perform electronic transactions. An example of this, which was not prevalent when HIPAA was being drafted, is the "cash and carry" type of health care now popping up all over the nation (e.g., small franchised clinics in retail stores). This may be slightly outside the scope of discussion of health information exchange, but those entities could very well become HIE participants as they obtain private data directly from patients.

I would be happy to entertain any questions you may have. I can be reached at (317) 402-0340 or vprescott@vprescott.com